ENUMERATIONS OF CAYLEY GRAPHS

DONGSEOK KIM, JIN HWAN KIM, JAEUN LEE, AND DIANJUN WANG

Abstract. We characterize the equivalence and the weak equivalence of Cayley graphs for a finite group $\mathcal{A}$. Using these characterizations, we find enumeration formulae of the equivalence classes and weak equivalence classes of Cayley graphs. As an application, we find the number of weak equivalence classes of circulant graphs.

1. Introduction

Let $\mathcal{A}$ be a finite group with identity e and let Ω be a set of generators for $\mathcal{A}$ with the properties that $\Omega = \Omega^{-1}$ and $e \notin \Omega$, where $\Omega^{-1} = \{x^{-1} \mid x \in \Omega\}$. The *Cayley graph* $C(\mathcal{A}, \Omega)$ is a simple graph whose vertex-set and edge-set are defined as follows:

$$V(C(\mathcal{A}, \Omega)) = \mathcal{A} \text{ and } E(C(\mathcal{A}, \Omega)) = \{\{g, h\} \mid g^{-1}h \in \Omega\}.$$

Because of its rich connections with broad range of areas, it has been in the center of the research in graph theory [1, 4, 14, 15]. Spectral estimations of Cayley graphs have been studied [2, 7]. It plays a key role in the study of the geometry of hyperbolic groups [9]. Recently, Li has found wonderful results on edge-transitive Cayley graphs [12, 13].

The Cayley graph $C(\mathcal{A}, \Omega)$ admits a natural $\mathcal{A}$-action, $\cdot : \mathcal{A} \times C(\mathcal{A}, \Omega) \to C(\mathcal{A}, \Omega)$ defined by $g \cdot g' = gg'$ for all $g, g' \in \mathcal{A}$. A graph G with an $\mathcal{A}$-action is called an *$\mathcal{A}$-graph*. So, every Cayley graph $C(\mathcal{A}, \Omega)$ is an $\mathcal{A}$-graph. A graph isomorphism $f : G \to H$ between two $\mathcal{A}$-graphs is *weak equivalence* if there exists a group automorphism $\alpha : \mathcal{A} \to \mathcal{A}$ such that $f(g \cdot u) = \alpha(g) \cdot f(u)$ for all $g \in \mathcal{A}$ and $u \in V(G)$. When α is the identity automorphism, we say that f is an *equivalence*. If there is a weak equivalence between $\mathcal{A}$-graphs G and H, we say G and H are *weak equivalent*. Similarly, if there is an equivalence between $\mathcal{A}$-graphs G and H, we say G and H are *equivalent*. For standard terms and notations, we refer to [8].

Enumerations of the equivalence classes and weak equivalence classes of some graphs have been studied [6, 11]. The purpose of this article is to enumerate the equivalence classes and weak equivalence classes of Cayley graphs for a finite group $\mathcal{A}$.

The outline of this paper is as follows. In section 2, we characterize the weak equivalence of Cayley graphs for a finite group $\mathcal{A}$. Using these characterizations, we find enumeration formulae of the equivalence classes and weak equivalence classes of Cayley graphs in section 3. As an application, we find the number of weak equivalence classes of circulant graphs in section 4.

2000 *Mathematics Subject Classification.* Primary 05C30; Secondary 05C25.

Key words and phrases. Cayley graphs, weak equivalences, equivalences, circulant graphs.

The third author was supported by Com^{2}MaC-KOSEF(R11-1999-054).

2. A characterization of Cayley graphs

Our definition of an weak equivalence between two Cayley graphs can be interpolated as a color-consistence and direction preserving graph isomorphism [8, Section 1.2.4].

Theorem 2.1. *Let $C(\mathcal{A}, \Omega)$ and $C(\mathcal{A}, \Omega')$ be two Cayley graphs. Then the followings are equivalent.*

(1) *$C(\mathcal{A}, \Omega)$ and $C(\mathcal{A}, \Omega')$ are weakly equivalent,*
(2) *There exists an isomorphism $\alpha : \mathcal{A} \to \mathcal{A}$ such that $\alpha(\Omega) = \Omega'$.*

Proof. (1) $\Rightarrow$ (2): Let $f : C(\mathcal{A}, \Omega) \to C(\mathcal{A}, \Omega')$ be a weak equivalence. Then there exists a group automorphism $\tau : \mathcal{A} \to \mathcal{A}$ such that $f(g) = \tau(g)f(e)$ for each $g \in \mathcal{A}$. Let $x \in \Omega$. Then $\{e, x\}$ is an edge in $C(\mathcal{A}, \Omega)$. Since $\{f(e), f(x)\}$ is an edge in $C(\mathcal{A}, \Omega')$, $f(e)^{-1}f(x) = f(e)^{-1}\tau(x)f(e)$ is an element of Ω'. Hence the map $\alpha : \mathcal{A} \to \mathcal{A}$ defined by $\alpha(g) = f(e)^{-1}\tau(g)f(e)$ is a group isomorphism such that $\alpha(\Omega) = \Omega'$.

(2) $\Rightarrow$ (1): Let $\alpha : \mathcal{A} \to \mathcal{A}$ be a group automorphism such that $\alpha(\Omega) = \Omega'$. We define $f : C(\mathcal{A}, \Omega) \to C(\mathcal{A}, \Omega')$ by $f(g) = \alpha(g)$. If $\{g, h\}$ is an edge in $C(\mathcal{A}, \Omega)$, then $g^{-1}h \in \Omega$ and $f(g)^{-1}f(h) = \alpha(g)^{-1}\alpha(h) = \alpha(g^{-1}h) \in \alpha(\Omega) = \Omega'$. Hence f is a graph isomorphism such that $f(gg') = \alpha(gg') = \alpha(g)\alpha(g') = \alpha(g)f(g')$, *i.e.*, f is a weak equivalence. □

By using a similar method in Theorem 2.1, we can have the following theorem.

Theorem 2.2. *Let $C(\mathcal{A}, \Omega)$ and $C(\mathcal{A}, \Omega')$ be two Cayley graphs. Then the followings are equivalent.*

(1) *$C(\mathcal{A}, \Omega)$ and $C(\mathcal{A}, \Omega')$ are equivalent,*
(2) *Ω and Ω' are conjugate in $\mathcal{A}$, i.e., there exists an element $g \in \mathcal{A}$ such that $g^{-1}\Omega g = \Omega'$.*

3. Enumeration formulae

For a finite group $\mathcal{A}$, let

$$G_m(\mathcal{A}) = \{\Omega \subset \mathcal{A} \,:\, \Omega^{-1} = \Omega, < \Omega >= \mathcal{A}, |\Omega| = m, e \notin \Omega\}.$$

Notice that $G_m(\mathcal{A})$ contains all equivalence classes of Cayley graphs $C(\mathcal{A}, \Omega)$ of degree m.

Let H be a group of group automorphisms of $\mathcal{A}$. H admits a natural action on $G_m(\mathcal{A})$ by $\alpha \cdot \Omega = \alpha(\Omega)$. By Theorem 2.1, $\mathcal{E}^w(\mathcal{A}, m)$, the number of weak equivalence classes of Cayley graphs $C(\mathcal{A}, \Omega)$ of degree m, is equal to the number of orbits of the $\mathrm{Aut}(\mathcal{A})$ action on $G_m(\mathcal{A})$, where $\mathrm{Aut}(\mathcal{A})$ is the group of all group isomorphisms of $\mathcal{A}$. Similarly, one can see that the number $\mathcal{E}(\mathcal{A}, m)$ of equivalence classes of Cayley graphs $C(\mathcal{A}, \Omega)$ of degree m is equal to the number of orbits of the $\mathrm{Inn}(\mathcal{A})$ action on $G_m(\mathcal{A})$ by Theorem 2.2, where $\mathrm{Inn}(\mathcal{A})$ is the group of all inner automorphisms of $\mathcal{A}$.

For any subset S of $\mathcal{A}$, let $O_2(S) = \{g \in S \,:\, g^2 = e, g \neq e\}$. We observe that

$$G_m(\mathcal{A}) = \bigcup_{k=0}^{\lfloor \frac{m}{2} \rfloor} \{\Omega \in G_m(\mathcal{A}) \,:\, |O_2(\Omega)| = m - 2k\} =: \bigcup_{k=0}^{\lfloor \frac{m}{2} \rfloor} G_{m,k}(\mathcal{A}).$$

This implies that

$$\mathcal{E}^w(\mathcal{A},m)=\sum_{k=0}^{\lfloor\frac{m}{2}\rfloor}|G_{m,k}(\mathcal{A})/\mathrm{Aut}(\mathcal{A})| \quad \text{and} \quad \mathcal{E}(\mathcal{A},m)=\sum_{k=0}^{\lfloor\frac{m}{2}\rfloor}|G_{m,k}(\mathcal{A})/\mathrm{Inn}(\mathcal{A})|.$$

Now, we aim to find a computational formula for the numbers $|G_{m,k}(\mathcal{A})/\mathrm{Aut}(\mathcal{A})|$ and $|G_{m,k}(\mathcal{A})/\mathrm{Inn}(\mathcal{A})|$. For each $x\in\mathcal{A}$, let $\overline{x}=\{x,x^{-1}\}$. Let us denote $\bar{G}_{m,k}(\mathcal{A})$, the set of all $(m-k)$-tuples $(\overline{x_1},\overline{x_2},\ldots,\overline{x_k},\overline{y_1},\ldots,\overline{y_{m-2k}})$ of distinct terms such that (1) $x_i^2\neq e,(i=1,2,\ldots,k)$, (2) $y_j^{-1}=y_j\neq e,(j=1,\ldots,m-2k)$, and (3) $\{x_1,x_2,\ldots,x_k,y_1,\ldots,y_{m-2k}\}$ generates $\mathcal{A}$.

Let S_k be the symmetric group on k letters and let $\mathcal{K}_k$ be the direct product $S_k\times S_{m-2k}$ of S_k and S_{m-2k}. Define an $\mathrm{Aut}(\mathcal{A})\times\mathcal{K}_k$ action on $\bar{G}_{m,k}(\mathcal{A})$ by

$$\begin{aligned}&(\alpha,\sigma,\tau)\cdot(\overline{x_1},\ldots,\overline{x_k},\overline{y_1},\ldots,\overline{y_{m-2k}})\\&=(\overline{\alpha(x_{\sigma^{-1}(1)})},\ldots,\overline{\alpha(x_{\sigma^{-1}(k)})},\overline{\alpha(y_{\tau^{-1}(1)})},\ldots,\overline{\alpha(y_{\tau^{-1}(m-2k)})}).\end{aligned}$$

Then it is not hard to show that

$$\begin{aligned}|\bar{G}_{m,k}(\mathcal{A})/\mathrm{Aut}(\mathcal{A})\times\mathcal{K}_k|&=|G_{m,k}(\mathcal{A})/\mathrm{Aut}(\mathcal{A})|,\\|\bar{G}_{m,k}(\mathcal{A})/\mathrm{Inn}(\mathcal{A})\times\mathcal{K}_k|&=|G_{m,k}(\mathcal{A})/\mathrm{Inn}(\mathcal{A})|.\end{aligned}$$

For a fixed element (α,σ,τ) in $\mathrm{Aut}(\mathcal{A})\times\mathcal{K}_k$, let $F_{(\alpha,\sigma,\tau)}(m,k,\mathcal{A})$ be the set all elements in $\bar{G}_{m,k}(\mathcal{A})$ such that $(\alpha,\sigma,\tau)\cdot(\overline{x_1},\ldots,\overline{x_k},\overline{y_1},\ldots,\overline{y_{m-2k}})=(\overline{x_1},\ldots,\overline{x_k},\overline{y_1},\ldots,\overline{y_{m-2k}})$. The following comes from the Burnside lemma.

Theorem 3.1. *Let $\mathcal{A}$ be a finite group and m be a positive integer. Then the number of weak equivalence classes of Cayley graphs $C(\mathcal{A},\Omega)$ of degree m, $\mathcal{E}^w(\mathcal{A},m)$, is*

$$\sum_{k=0}^{\lfloor\frac{m}{2}\rfloor}|G_{m,k}(\mathcal{A})/\mathrm{Aut}(\mathcal{A})|=\sum_{k=0}^{\lfloor\frac{m}{2}\rfloor}\frac{\sum_{(\alpha,\sigma,\tau)\in\mathrm{Aut}(\mathcal{A})\times\mathcal{K}_k}|F_{(\alpha,\sigma,\tau)}(m,k,\mathcal{A})|}{|\mathrm{Aut}(\mathcal{A})|\,k!(m-2k)!},$$

and the number of equivalence classes of Cayley graphs $C(\mathcal{A},\Omega)$ of degree m, $\mathcal{E}(\mathcal{A},m)$, is

$$\sum_{k=0}^{\lfloor\frac{m}{2}\rfloor}|G_{m,k}(\mathcal{A})/\mathrm{Inn}(\mathcal{A})|=\sum_{k=0}^{\lfloor\frac{m}{2}\rfloor}\frac{\sum_{(\alpha,\sigma,\tau)\in\mathrm{Inn}(\mathcal{A})\times\mathcal{K}_k}|F_{(\alpha,\sigma,\tau)}(m,k,\mathcal{A})|}{|\mathrm{Inn}(\mathcal{A})|\,k!(m-2k)!}.$$

Now, we will compute $|F_{(\alpha,\sigma,\tau)}(m,k,\mathcal{A})|$. For each subgroup $\mathcal{S}$ of $\mathcal{A}$ such that $\alpha(\mathcal{S})=\mathcal{S}$, let us denote $\tilde{G}_{m,k}(\mathcal{S})$ the set of all $(m-k)$-tuples $(\overline{x_1},\overline{x_2},\ldots,\overline{x_k},\overline{y_1},\ldots,\overline{y_{m-2k}})$ of distinct elements in $\mathcal{S}$ such that (1) $x_i^2\neq e,(i=1,2,\ldots,k)$, and (2) $y_j^{-1}=y_j\neq e,(j=1,\ldots,m-2k)$. Then $\tilde{G}_{m,k}(\mathcal{S})$ is also an $\mathrm{Aut}(\mathcal{A})\times\mathcal{K}_k$ set. Let $\tilde{F}_{(\alpha,\sigma,\tau)}(m,k,\mathcal{S})$ be the set of all elements in $\tilde{G}_{m,k}(\mathcal{S})$ such that $(\alpha,\sigma,\tau)\cdot(\overline{x_1},\ldots,\overline{x_k},\overline{y_1},\ldots,\overline{y_{m-2k}})=(\overline{x_1},\ldots,\overline{x_k},\overline{y_1},\ldots,\overline{y_{m-2k}})$. It follows from the Möbius inversion that

$$|F_{(\alpha,\sigma,\tau)}(m,k,\mathcal{A})|=\sum_{\mathcal{S}\leq\mathcal{A},\alpha(\mathcal{S})=\mathcal{S}}\mu(\mathcal{S})\,|\tilde{F}_{(\alpha,\sigma,\tau)}(m,k,\mathcal{S})|,$$

where μ is the Möbius function which assigns an integer $\mu(\mathcal{S})$ to each subgroup $\mathcal{S}$ of $\mathcal{A}$ such that $\alpha(\mathcal{S}) = \mathcal{S}$ by the recursive formula

$$\sum_{\mathcal{S}' \geq \mathcal{S}} \mu(\mathcal{S}') = \delta_{\mathcal{S},\mathcal{A}} = \begin{cases} 1 \text{ if } \mathcal{S} = \mathcal{A}, \\ 0 \text{ if } \mathcal{S} < \mathcal{A}. \end{cases}$$

Let $\mathcal{S}$ be a subgroup of $\mathcal{A}$. We consider $\mathrm{Aut}(\mathcal{A}) \times S_k$ action on the set $\tilde{G}_{2k,k}(\mathcal{S})$ and $\mathrm{Aut}(\mathcal{S}) \times S_{m-2k}$ action on the set $\tilde{G}_{m-2k,0}(\mathcal{S})$. Then

$$|\tilde{F}_{(\alpha,\sigma,\tau)}(m,k,\mathcal{S})| = |\tilde{F}_{(\alpha,\sigma)}(2k,k,\mathcal{S})|\,|\tilde{F}_{(\alpha,\tau)}(m-2k,0,\mathcal{S})|,$$

for any subgroup $\mathcal{S}$ of $\mathcal{A}$. To complete the computation, we need computational formulae for these two numbers $|\tilde{F}_{(\alpha,\sigma)}(2k,k,\mathcal{S})|$ and $|\tilde{F}_{(\alpha,\tau)}(m-2k,0,\mathcal{S})|$ for a subgroup $\mathcal{S}$ of $\mathcal{A}$ such that $\alpha(\mathcal{S}) = \mathcal{S}$. For $\alpha \in \mathrm{Aut}(\mathcal{A})$ and a positive integer n, let

$$\tilde{F}_{(\alpha,n)}(\mathcal{S}) = \{g \in \mathcal{S} : g \neq g^{-1}, \alpha^n(g) = g, \alpha^l(g) \neq g \text{ and } \alpha^l(g) \neq g^{-1}\,(l < n)\},$$

$$\tilde{I}_{(\alpha,n)}(\mathcal{S}) = \{g \in \mathcal{A} : g \neq g^{-1}, \alpha^n(g) = g^{-1}, \alpha^l(g) \neq g \text{ and } \alpha^l(g) \neq g^{-1}\,(l < n)\},$$

and

$$\tilde{F}^o_{(\alpha,n)}(\mathcal{S}) = \{g \in \mathcal{S} : g^{-1} = g \neq e, \alpha^n(g) = g \text{ and } \alpha^l(g) \neq g (l < n)\}.$$

For a fixed element $\sigma \in S_n$, let $j_k(\sigma)$ be the number of disjoint k cycles in the factorization of σ into disjoint cycles, *i.e.*, $\sigma = \sigma_{j_1(\sigma)} \cdots \sigma_{j_n(\sigma)}$, where $\sigma_{j_k(\sigma)}$ is the product of $j_k(\sigma)$ disjoint k cycles.

Lemma 3.2. *Let $\alpha \in \mathrm{Aut}(\mathcal{A})$, $\sigma \in S_k$ and $\tau \in S_{m-2k}$. Then for any subgroup $\mathcal{S}$ of $\mathcal{A}$ such that $\alpha(\mathcal{S}) = \mathcal{S}$, we have*

$$|\tilde{F}_{(\alpha,\sigma,\tau)}(m,k,\mathcal{S})| = \prod_{r=1}^{k} \prod_{s=0}^{j_r(\sigma)-1} \left(\frac{|\tilde{F}_{(\alpha,r)}(\mathcal{S})| + |\tilde{I}_{(\alpha,r)}(\mathcal{S})|}{2} - rs \right) \prod_{l=1}^{m-2k} \prod_{t=0}^{j_l(\tau)-1} \left(|\tilde{F}^o_{(\alpha,l)}(\mathcal{S})| - lt \right).$$

In particular, if $|\mathcal{A}|$ is odd, then we have

$$|\tilde{F}_{(\alpha,\sigma,\tau)}(m,k,\mathcal{S})| = \begin{cases} \displaystyle\prod_{r=1}^{k} \prod_{s=0}^{j_r(\sigma)-1} \left(\frac{|\tilde{F}_{(\alpha,r)}(\mathcal{S})| + |\tilde{I}_{(\alpha,r)}(\mathcal{S})|}{2} - rs \right) & \text{if } m \text{ is even and } k = \frac{m}{2}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Notice that $(\overline{x_1}, \ldots, \overline{x_k})$ is an element of $\tilde{F}_{(\alpha,\sigma)}(2k,k,\mathcal{S})$ if and only if $\overline{x_i} = \overline{\alpha(x_{\sigma^{-1}(i)})}$ for each $i = 1, 2, \ldots, k$. It means that if the length of the orbit of i under the $< \sigma >$ is r, then $x_i = \alpha^r(x_i)$ or $x_i^{-1} = \alpha^r(x_i)$, *i.e.*, $x_i \in \tilde{F}_{(\alpha,r)}(\mathcal{S}) \cup \tilde{I}_{(\alpha,r)}(\mathcal{S})$. Since the number of orbits of length r is $j_r(\sigma)$, the set $\{x_i, x_i^{-1}, \alpha(x_{\sigma(i)}), \alpha(x_{\sigma(i)}^{-1}), \ldots, \alpha(x_{\sigma^{r-1}(i)}), \alpha(x_{\sigma^{r-1}(i)}^{-1})\}$ contains $2r$ numbers of elements in $\tilde{F}_{(\alpha,r)}(\mathcal{S}) \cup \tilde{I}_{(\alpha,r)}(\mathcal{S})$, and $\{\overline{x_i}, \overline{\alpha(x_{\sigma(i)})}, \ldots, \overline{\alpha(x_{\sigma^{r-1}(i)})}\} = \{\overline{x_i^{-1}}, \overline{\alpha(x_{\sigma(i)}^{-1})}, \ldots, \overline{\alpha(x_{\sigma^{r-1}(i)}^{-1})}\}$. Since $F_{(\alpha,r)}(\mathcal{S})$ and $I_{(\alpha,r)}(\mathcal{S})$ are disjoint, we have

$$|\tilde{F}_{(\alpha,\sigma)}(2k,k,\mathcal{S})| = \prod_{r=1}^{k} \prod_{s=0}^{j_r(\sigma)-1} \left(\frac{|\tilde{F}_{(\alpha,r)}(\mathcal{S})| + |\tilde{I}_{(\alpha,r)}(\mathcal{S})|}{2} - rs \right).$$

Similarly, we can show that

$$|\tilde{F}_{(\alpha,\tau)}(m-2k,0,\mathcal{S})| = \prod_{l=1}^{m-2k}\prod_{t=0}^{j_l(\tau)-1}\left(|\tilde{F}^o_{(\alpha,r)}(\mathcal{S})| - lt\right).$$

Notice that if $|\mathcal{A}|$ is odd, then $|\tilde{F}^o_{\alpha^r}(\mathcal{S})| = 0$. It completes the proof. □

We observe that if σ_1 and σ_2 are conjugate in S_k, then $|\tilde{F}_{(\alpha,\sigma_1)}(2k,k,\mathcal{S})| = |\tilde{F}_{(\alpha,\sigma_2)}(2k,k,\mathcal{S})|$ for any automorphism α of $\mathcal{A}$ and any subgroup $\mathcal{S}$ of $\mathcal{A}$ with $\alpha(\mathcal{S}) = \mathcal{S}$. Similarly, we can see that if τ_1 and τ_2 are conjugate in S_{m-2k}, then $|\tilde{F}^o_{(\alpha,\tau_1)}(m-2k,0,\mathcal{S})| = |\tilde{F}_{(\alpha,\tau_2)}(m-2k,0,\mathcal{S})|$ for any automorphism α of $\mathcal{A}$ and any subgroup $\mathcal{S}$ of $\mathcal{A}$ with $\alpha(\mathcal{S}) = \mathcal{S}$. Moreover, the number of elements in S_m which are conjugate to σ is equal to

$$\frac{m!}{j_1(\sigma)!2^{j_2(\sigma)}j_2(\sigma)!\cdots m^{j_m(\sigma)}j_m(\sigma)!}.$$

Now, by the fact that $j_1(\sigma)+2j_2(\sigma)+\cdots+mj_m(\sigma) = m$, Theorem 3.1 can be reformulated as follows.

Theorem 3.3. *Let $\mathcal{A}$ be a finite group and m be a positive integer. Then we have*

$$\begin{aligned}
&|\mathrm{Aut}(\mathcal{A})|\ \mathcal{E}^w(\mathcal{A},m)\\
&=\sum_{k=0}^{\lfloor\frac{m}{2}\rfloor}\sum_{\alpha\in\mathrm{Aut}(\mathcal{A})}\sum_{\mathcal{S}\le\mathcal{A},\alpha(\mathcal{S})=\mathcal{S}}\mu(\mathcal{S})\left(\sum_{j_1+2j_2+\cdots+kj_k=k}\frac{\prod_{r=1}^{k}\prod_{t=0}^{j_r-1}\left(\frac{|\tilde{F}_{\alpha^r}(\mathcal{S})|+|\tilde{I}_{\alpha^r}(\mathcal{S})|}{2}-rs\right)}{j_1!2^{j_2}j_2!\cdots k^{j_k}j_k!}\right)\\
&\qquad\times\left(\sum_{j_1+2j_2+\cdots+(m-2k)j_{m-2k}=m-2k}\frac{\prod_{l=1}^{m-2k}\prod_{t=0}^{j_l-1}\left(|\tilde{F}^o_{\alpha^l}(\mathcal{S})|-lt\right)}{j_1!2^{j_2}j_2!\cdots(m-2k)^{j_{m-2k}}j_{m-2k}!}\right),
\end{aligned}$$

and

$$\begin{aligned}
&|\mathrm{Inn}(\mathcal{A})|\ \mathcal{E}(\mathcal{A},m)\\
&=\sum_{k=0}^{\lfloor\frac{m}{2}\rfloor}\sum_{\alpha\in\mathrm{Inn}(\mathcal{A})}\sum_{\mathcal{S}\le\mathcal{A},\alpha(\mathcal{S})=\mathcal{S}}\mu(\mathcal{S})\left(\sum_{j_1+2j_2+\cdots+kj_k=k}\frac{\prod_{r=1}^{k}\prod_{t=0}^{j_r-1}\left(\frac{|\tilde{F}_{\alpha^r}(\mathcal{S})|+|\tilde{I}_{\alpha^r}(\mathcal{S})|}{2}-rs\right)}{j_1!2^{j_2}j_2!\cdots k^{j_k}j_k!}\right)\\
&\qquad\times\left(\sum_{j_1+2j_2+\cdots+(m-2k)j_{m-2k}=m-2k}\frac{\prod_{l=1}^{m-2k}\prod_{t=0}^{j_l-1}\left(|\tilde{F}^o_{\alpha^l}(\mathcal{S})|-lt\right)}{j_1!2^{j_2}j_2!\cdots(m-2k)^{j_{m-2k}}j_{m-2k}!}\right).
\end{aligned}$$

Now, we will compute $|\tilde{F}_{(\alpha,r)}(\mathcal{S})|$, $|\tilde{I}_{(\alpha,r)}(\mathcal{S})|$, and $|\tilde{F}^o_{(\alpha,r)}(\mathcal{S})|$. For convenience, let

$$\begin{aligned}
\tilde{\tilde{F}}_{(\alpha,r)}(\mathcal{S}) &= \{g \in \mathcal{S} \,:\, \alpha^r(g) = g, g^{-1} \neq g\},\\
\tilde{\tilde{I}}_{(\alpha,r)}(\mathcal{S}) &= \{g \in \mathcal{S} \,:\, \alpha^r(g) = g^{-1}, g^{-1} \neq g\},\\
\tilde{\tilde{F}}^o_{(\alpha,r)}(\mathcal{S}) &= \{g \in \mathcal{S} \,:\, \alpha^r(g) = g, g^{-1} = g \neq e\}.
\end{aligned}$$

Lemma 3.4. *Let $\mathcal{A}$ be a finite group and let α be an automorphism on $\mathcal{A}$ of order $|<\alpha>|$. Then for any positive integer r and any subgroup $\mathcal{S}$ of $\mathcal{A}$ such that $\alpha(\mathcal{S}) = \mathcal{S}$, we have*

$$|\tilde{F}_{\alpha^r}(\mathcal{S})| = \begin{cases} \displaystyle\sum_{d|r} \mu\left(\frac{r}{d}\right) \left|\tilde{\tilde{F}}_{\alpha^d}(\mathcal{S})\right| & \text{if } r \text{ is a divisor of } |<\alpha>| \text{ and odd,}\\ \displaystyle\sum_{d|r} \mu\left(\frac{r}{d}\right) \left|\tilde{\tilde{F}}_{\alpha^d}(\mathcal{S})\right| - |\tilde{I}_{\alpha^{\frac{r}{2}}}(\mathcal{S})| & \text{if } r \text{ is a divisor of } |<\alpha>| \text{ and even,}\\ 0 & \text{if } r \text{ is not a divisor of } |<\alpha>|, \end{cases}$$

$$|\tilde{F}^o_{\alpha^r}(\mathcal{S})| = \begin{cases} \displaystyle\sum_{d|r} \mu\left(\frac{r}{d}\right) \left|\tilde{\tilde{F}}^o_{\alpha^d}(\mathcal{S})\right| & \text{if } r \text{ is a divisor of } |<\alpha>|,\\ 0 & \text{otherwise,} \end{cases}$$

and

$$|\tilde{I}_{\alpha^r}(\mathcal{S})| = \begin{cases} \displaystyle\sum_{d|r \text{ and } \frac{r}{d} \text{ is odd}} \mu\left(\frac{r}{d}\right) \left|\tilde{\tilde{I}}_{\alpha^d}(\mathcal{S})\right| & \text{if } 2r \text{ is a divisor of } |<\alpha>|,\\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $x \in \mathcal{S}$ such that $\alpha^r(x) = x$ and $x \neq x^{-1}$. If $\alpha^l(x) = x$ for some l, then $\alpha^d(x) = x$, where $d = (r, l)$ is the greatest common divisor of r and l. It implies that if $\alpha^l(x) = x$ then $x \in \tilde{\tilde{F}}_{\alpha^d}(\mathcal{S})$ for some divisor d of r. Since $\alpha^{(r,|<\alpha>|)}(x) = x$, $|\tilde{F}_{\alpha^r}(\mathcal{S})| \neq 0$ when $r = (r, |<\alpha>|)$, *i.e.*, r is a divisor of $|<\alpha>|$.

If $\alpha^l(x) = x^{-1}$ for $l < r$, then $\alpha^{2l}(x) = x$ and hence $\alpha^{(r,2l)}(x) = x$. It implies that if $d = (r, 2l) < r$ then $x \in \tilde{\tilde{F}}_{\alpha^d}(\mathcal{S})$, and if $d = (r, 2l) = r$, then $2l = r$ and $x \in \tilde{\tilde{I}}_{\alpha^{\frac{r}{2}}}(\mathcal{S})$. Now, we can see that

$$\tilde{F}_{\alpha^r}(\mathcal{S}) = \tilde{\tilde{F}}_{\alpha^r}(\mathcal{S}) - \left(\bigcup_{d|r \text{ and } d\neq r} \tilde{\tilde{F}}_{\alpha^d}(\mathcal{S}) \cup \tilde{\tilde{I}}_{\alpha^{\frac{r}{2}}}(\mathcal{S}) \right).$$

Notice that if $\alpha^s(x) = x$ and $s|t$ then $\alpha^t(x) = x$, *i.e.*, $\tilde{\tilde{F}}_{\alpha^s}(\mathcal{S}) \subset \tilde{\tilde{F}}_{\alpha^t}(\mathcal{S})$ for each s and t with $s|t$. Since

$$\tilde{\tilde{I}}_{\alpha^{\frac{r}{2}}}(\mathcal{S}) - \bigcup_{d|r \text{ and } d\neq r} \tilde{\tilde{F}}_{\alpha^d}(\mathcal{S}) = \tilde{I}_{\alpha^{\frac{r}{2}}}(\mathcal{S}),$$

we have

$$|\tilde{F}_{\alpha^r}(\mathcal{S})| = \begin{cases} \sum_{d|r} \mu\left(\frac{r}{d}\right) \left|\tilde{\tilde{F}}_{\alpha^d}(\mathcal{S})\right| & \text{if } r \text{ is a divisor of } |<\alpha>| \text{ and odd,} \\ \sum_{d|r} \mu\left(\frac{r}{d}\right) \left|\tilde{\tilde{F}}_{\alpha^d}(\mathcal{S})\right| - |\tilde{I}_{\alpha^{\frac{r}{2}}}(\mathcal{S})| & \text{if } r \text{ is a divisor of } |<\alpha>| \text{ and even,} \\ 0 & \text{if } r \text{ is not a divisor of } |<\alpha>|. \end{cases}$$

By a method similar to the computation of $|\tilde{F}_{\alpha^r}(\mathcal{S})|$, we have

$$|\tilde{F}^o_{\alpha^r}(\mathcal{S})| = \sum_{d|r} \mu\left(\frac{r}{d}\right) |\tilde{\tilde{F}}^o_{\alpha^d}(\mathcal{S})|.$$

Let $x \in \mathcal{S}$ such that $\alpha^r(x) = x^{-1}$ and $x \neq x^{-1}$. If $\alpha^l(x) = x$ for some l, then $\alpha^{(2r,l)}(x) = x$. In particular, $\alpha^{(2r,|<\alpha>|)}(x) = x$. This implies that $|\tilde{I}_{\alpha^r}(\mathcal{S})| \neq 0$ when $2r = (2r, |<\alpha>|)$, *i.e.*, $2r$ is a divisor of $|<\alpha>|$. For $l \leq r$, Put $d = (2r, l)$. Then $\alpha^d(x) = x$. If d is a divisor of r, then $x = \alpha^{d\frac{r}{d}}(x) = \alpha^r(x) = x^{-1}$. Since $x \neq x^{-1}$, d can not be a divisor of r. Since $d|2r$, d is even and $\dfrac{2r}{d}$ is odd. Hence, $x^{-1} = \alpha^r(x) = \alpha^{\frac{d}{2}\frac{2r}{d}}(x) = \alpha^{\frac{d}{2}}(x)$, *i.e.*, $\alpha^{d'}(x) = x^{-1}$ for some $d'|r$ and $\dfrac{r}{d'}$ is odd. If $\alpha^l(x) = x^{-1}$ for some $l \leq r$, then $\alpha^{(2r,2l)}(x) = x$. Put $(2r, 2l) = 2(r, l) = 2d$. Then $\alpha^{2d}(x) = x$ and $x^{-1} = \alpha^r(x) = \alpha^{d\frac{r}{d}}(x)$. Since $x \neq x^{-1}$, $\dfrac{r}{d}$ is odd and $\alpha^d(x) = x^{-1}$. Now, we can see that

$$\tilde{I}_{\alpha^r}(\mathcal{S}) = \tilde{\tilde{I}}_{\alpha^r}(\mathcal{S}) - \bigcup_{d|r,\ d\neq r \text{ and } \frac{r}{d} \text{ is odd}} \tilde{\tilde{I}}_{\alpha^d}(\mathcal{S}),$$

and hence,

$$|\tilde{I}_{\alpha^r}(\mathcal{S})| = \sum_{d|r \text{ and } \frac{r}{d} \text{ is odd}} \mu\left(\frac{r}{d}\right) |\tilde{\tilde{I}}_{\alpha^d}(\mathcal{S})|.$$

It completes the proof. □

Let $\mathcal{A}$ be a finite abelian group. Then $\mathrm{Inn}(\mathcal{A}) = \{id_{\mathcal{A}}\}$. Let $\mathcal{S}$ be a subgroup of $\mathcal{A}$. Then $|\tilde{F}_1(\mathcal{S})| + |\tilde{I}_1(\mathcal{S})| = |\mathcal{S}| - |O_2(\mathcal{S})| - 1$ and $|\tilde{F}^o_1(\mathcal{S}) = |O_2(\mathcal{S})|$. Now, by Theorem 3.3 and Lemma 3.4, we have the following corollary.

Corollary 3.5. *Let $\mathcal{A}$ be a finite abelian group and m be a positive integer. Then the number of weak equivalence classes of Cayley graphs $C(\mathcal{A}, \Omega)$ of degree m, $\mathcal{E}(\mathcal{A}, m)$ is*

$$\sum_{k=0}^{\lfloor \frac{m}{2} \rfloor} \sum_{\mathcal{S}\leq\mathcal{A}} \mu(\mathcal{S}) \binom{\frac{1}{2}(|\mathcal{S}| - |O_2(\mathcal{S})| - 1)}{k} \binom{|O_2(\mathcal{S})|}{m-2k},$$

where $O_2(\mathcal{S}) = \{g \in \mathcal{S} \ : \ g^2 = e, g \neq e\}$. In particular, if $\mathcal{A}$ is odd, then

$$\mathcal{E}(\mathcal{A}, m) = \begin{cases} \sum_{\mathcal{S}\leq\mathcal{A}} \mu(\mathcal{S}) \binom{\frac{1}{2}(|\mathcal{S}| - 1)}{\frac{m}{2}} & \text{if } m \text{ is even,} \\ 0 & \text{if } m \text{ is odd.} \end{cases}$$

4. Applications to circulant graphs

Let $\mathbb{Z}_n$ be the additive cyclic group of order n. A connected *circulant graph* is a Cayley graph $C(\mathbb{Z}_n, \Omega)$ for the cyclic group $\mathbb{Z}_n$ of order n. Let p be a prime number. Two circulant graphs for a cyclic group $\mathbb{Z}_p$ are isomorphic if and only if they are weakly equivalent [5]. So, the number $\mathcal{E}^w(\mathbb{Z}_p, m)$ of weak equivalence classes and the number of isomorphism classes of Cayley graphs $C(\mathbb{Z}_p, \Omega)$ of degree m are equal.

We identify $\mathrm{Aut}(\mathbb{Z}_n)$ with the set of all elements of $\mathbb{Z}_n$ which are relatively prime to n, that is, the set $\{\alpha \in \mathbb{Z}_n : (\alpha, n) = 1\}$. Notice that $\mathrm{Aut}(\mathbb{Z}_n)$ has $\phi(n)$ elements, where ϕ is the Euler function. Notice that the number of elements g in $\mathbb{Z}_n$ such that $g = -g$ is one if n is odd or two if n is even. Moreover, such elements are fixed by every automorphism α of $\mathbb{Z}_n$, *i.e.*, $\alpha(g) = g$. Since α^r is also an automorphism for any automorphism α and any integer r, we have

$$|\tilde{F}^o_{\alpha^r}(\mathbb{Z}_n)| = \begin{cases} 1 & \text{if } r = 1 \text{ and } n \text{ is even,} \\ 0 & \text{otherwise.} \end{cases}$$

Now, we aim to compute $|\tilde{F}_{\alpha^r}(\mathbb{Z}_n)|$ and $|\tilde{I}_{\alpha^r}(\mathbb{Z}_n)|$. By Lemma 3.4, it is sufficient to compute $|\tilde{\tilde{F}}_{\alpha^r}(\mathbb{Z}_n)|$ and $|\tilde{\tilde{I}}_{\alpha^r}(\mathbb{Z}_n)|$. Let α be an automorphism and let r be an integer. Then $g \in \tilde{\tilde{F}}_{\alpha^r}(\mathbb{Z}_n)$ if and only if $\alpha^r(g) = g$ and $2g \neq 0$, *i.e.*, $(\alpha^r - 1)g = 0$ and $2g \neq 0$, and $g \in \tilde{\tilde{I}}_{\alpha^r}(\mathbb{Z}_n)$ if and only if $\alpha^r(g) = -g$ and $2g \neq 0$, *i.e.*, $(\alpha^r + 1)g = 0$ and $2g \neq 0$. Hence we have the following lemma.

Lemma 4.1. *Let $\alpha \in \mathbb{Z}_n$ such that $(\alpha, n) = 1$ and for any natural number r, we have*

$$|\tilde{\tilde{F}}_{\alpha^r}(\mathbb{Z}_n)| = \begin{cases} (\alpha^r - 1, n) - 1 & \text{if } n \text{ is odd,} \\ (\alpha^r - 1, n) - 2 & \text{if } n \text{ is even,} \end{cases}$$

$$|\tilde{\tilde{I}}_{\alpha^r}(\mathbb{Z}_n)| = \begin{cases} (\alpha^r + 1, n) - 1 & \text{if } n \text{ is odd,} \\ (\alpha^r + 1, n) - 2 & \text{if } n \text{ is even.} \end{cases}$$

Corollary 4.2. *Let p be an odd prime and let $\alpha \in \mathbb{Z}_p$ such that $(\alpha, p) = 1$. Then for any natural number r, we have*

$$|\tilde{F}_{\alpha^r}(\mathbb{Z}_p)| = \begin{cases} p - 1 & \text{if } r \text{ is odd, the order of } \alpha \text{ is } r \text{ and } r|(p-1), \\ 0 & \text{otherwise,} \end{cases}$$

and

$$|\tilde{I}_{\alpha^r}(\mathbb{Z}_p)| = \begin{cases} p - 1 & \text{if order of } \alpha \text{ is } 2r \text{ and } r|(\dfrac{p-1}{2}), \\ 0 & \text{otherwise.} \end{cases}$$

From Corollary 4.2, we can see that

$$|\tilde{F}_{\alpha^r}(\mathbb{Z}_p)| + |\tilde{I}_{\alpha^r}(\mathbb{Z}_p)| = \begin{cases} p - 1 & \text{if } r \text{ is odd, order of } \alpha \text{ is } r \text{ and } r|(p-1), \\ p - 1 & \text{if order of } \alpha \text{ is } 2r \text{ and } r|(\dfrac{p-1}{2}), \\ 0 & \text{otherwise.} \end{cases}$$

Notice that $\bar{G}_{m,k}(\mathbb{Z}_p) \neq \emptyset$ if and only if $m \leq \frac{p-1}{2}$, m is even, and $k = \frac{m}{2}$. From now on, we only consider $m \leq \frac{p-1}{2}$. Let $\sigma \in S_{\frac{m}{2}}$ and let $\alpha \in \mathrm{Aut}(\mathbb{Z}_p)$. Then

$$|\tilde{F}_{(\alpha,\sigma)}| = \begin{cases} \prod_{t=0}^{\frac{m}{2l}-1} \left(\frac{p-1}{2} - rt\right) & \text{if } j_l(\sigma) = \frac{m}{2l},\ |<\alpha>| = l,\ l|(\frac{p-1}{2}),\text{ and } l \text{ is odd,} \\ \prod_{t=0}^{\frac{m}{2l}-1} \left(\frac{p-1}{2} - rt\right) & \text{if } j_l(\sigma) = \frac{m}{2l},\ |<\alpha>| = 2l,\text{ and } l|(\frac{p-1}{2}). \end{cases}$$

Notice that $\mathbb{Z}_p$ has no nontrivial subgroup, and that the order of each element in $\mathrm{Aut}(\mathbb{Z}_p)$ is a divisor of $p-1$ and $|\{\alpha \in \mathrm{Aut}(\mathbb{Z}_p) : |<\alpha>| = k\}| = \phi(k)$ for each $k|(p-1)$. By summarizing these together with Theorem 3.3, we find the following theorem.

Theorem 4.3. *Let p be a prime number and let $m \leq \frac{p-1}{2}$. Then*

$$(p-1)\,\mathcal{E}^w(\mathbb{Z}_p, m) = \sum_{k|(\frac{p-1}{2},\frac{m}{2}) \text{ and } k \text{ is odd}} \phi(k)\, \frac{\prod_{t=0}^{\frac{m}{2k}-1} \left(\frac{p-1}{2} - kt\right)}{k^{\frac{m}{2k}} \left(\frac{m}{2k}\right)!} + \sum_{k|(\frac{p-1}{2},\frac{m}{2})} \phi(2k)\, \frac{\prod_{t=0}^{\frac{m}{2k}-1} \left(\frac{p-1}{2} - kt\right)}{k^{\frac{m}{2k}} \left(\frac{m}{2k}\right)!}.$$

In particular, if $\frac{m}{2}$ or $\frac{p-1}{2}$ is odd, then

$$(p-1)\,\mathcal{E}^w(\mathbb{Z}_p, m) = 2 \sum_{k|(\frac{p-1}{2},\frac{m}{2})} \phi(k)\, \frac{\prod_{t=0}^{\frac{m}{2k}-1} \left(\frac{p-1}{2} - kt\right)}{k^{\frac{m}{2k}} \left(\frac{m}{2k}\right)!}.$$

Moreover, if $(\frac{p-1}{2}, \frac{m}{2}) = 1$, then

$$\mathcal{E}^w(\mathbb{Z}_p, m) = \binom{\frac{1}{2}(p-3)}{\frac{m}{2}}.$$

References

[1] L. Branković, M. Miller, J. Plesnik, J. Ryan and J. Širáň, *A note on constructing large Cayley graphs of given degree and diameter by voltage assignments*, Electronic Journal of Combinatorics 5 (1998), #R9.

[2] S. Cioabă, *Closed walks and eigenvalues of abelian Cayley graphs*, To appear in C. R. Acad. Sci. Paris, Ser. I.

[3] I. Dejter and O. Serr, *Efficient dominating sets in Cayley graphs*, Discrete Applied Mathematics, 129(2) (2003), 319–328.
[4] C. Droms, B. Servatius and H. Servatius, *Connectivity and planarity of Cayley Graphs*, Beitrage zur Algebra und Geometrie Contributions to Algebra and Geometry Volume 39(2) (1998), 269–282.
[5] B. Elspas and J. Turner, *Graphs with circulant adjacency matrics*, Journal of Combinatorial Theory 9 (1990), 297–307.
[6] R. Feng, J. Y. Kim, J. H. Kwak and J. Lee, *Isomorphism classes of concrete graph coverings*, SIAM J. Discrete Math. 11 (1998), 265–272.
[7] J. Friedmana, R. Murtyc and J-P. Tillichd, *Spectral estimates for abelian Cayley graphs*, Journal of Combinatorial Theory, Series B 96 (2006), 111–121.
[8] J. L. Gross and T. W. Tucker, Topological graph theory, Wiley, New York, 1987.
[9] I. Kapovich, *The geometry of relative Cayley graphs for subgroups of hyperbolic groups*, preprint, arXiv:math.GR/0201045.
[10] Y. Katznelson, *Chromatic numbers of Cayley graphs on $\mathbb{Z}$ and recurrence*, Combinatorica 21(2) (2001), 211–219.
[11] J. H. Kwak and J. Lee, *Isomorphism classes of bipartite cycle permutation graphs*, ARS Combin. 50 (1998), 139–148.
[12] C. H. Li, *Finite edge-transitive Cayley graphs and rotary Cayley maps*, Trans. AMS. 358(10) (2006), 4605–4635.
[13] C. H. Li and Z. P. Lu, *Tetravalent edge-transitive Cayley graphs with odd number of vertices*, Journal of Combinatorial Theory Series B 96(1) (2006), 164–181.
[14] I. Pak and R. Radoičić, *Hamiltonian paths in Cayley graphs*, preprint.
[15] J. Rosenhouse, *Isoperimetric numbers of Cayley graphs arising from generalized dihedral groups*, Journal of Combinatorial Mathematics and Combinatorial Computing 42 (2002), 127–138.

Department of Mathematics, Yeungnam University, Kyongsan, 712-749, Korea
E-mail address: dongseok@yu.ac.kr

Mathematics Education, Yeungnam University, Kyongsan, 712-749, Korea
E-mail address: kimjh@ynucc.yeungnam.ac.kr

Department of Mathematics, Yeungnam University, Kyongsan, 712-749, Korea
E-mail address: julee@yu.ac.kr

Department of Mathematical Sciences, Tsinghua University, Beijing, China
E-mail address: djwang@math.tsinghua.edu.cn